IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

"Optimization and Evaluation of Blockchain-Based Authentication Systems with Zero-Knowledge Proofs and Multi-Factor Authentication"

Prof. Namrata Jangam
Computer Engineering
VPSCET Lonavala
Project Guide
namratajangam08@gmail.com

Hazra R. Shaikh
Computer Engineering
VPSCET Lonavala
Student
hazrashaikh64@gmail.com

Zainab E. Shaikh
Computer Engineering
VPSCET Lonavala
Student
zs509414@gmail.com

Shardha S. Pawar
Computer Engineering
VPSCET Lonavala
Student
pshradha8011@gmail.com

Rutuja K. Rahinj
Computer Engineering
VPSCET Lonavala
Student
rutujarahinj50@gmail.com

Abstract: Centralized authentication systems suffer from security risks such as single points of failure, password theft, and privacy leakage. Blockchain-based authentication provides decentralization and trust but faces challenges related to performance, cost, and scalability. This paper presents the implementation of a secure authentication framework combining Zero-Knowledge Proofs (ZKPs) and Multi-Factor Authentication (MFA) to enhance privacy and security. ZKPs enable identity verification without revealing sensitive user data, while MFA strengthens resistance against common attacks. The proposed system utilizes off-chain computation with on-chain verification to reduce latency and gas costs. Experimental analysis demonstrates improved efficiency, security, and user experience. The framework is suitable for applications requiring high security such as banking, healthcare, and IoT systems.

Keywords: Blockchain Authentication, Zero-Knowledge Proofs, Multi-Factor Authentication, Privacy Preservation, Off-chain Computation, Smart Contracts, Identity Verification.

I. INTRODUCTION

The rapid growth of connected devices and digital services has made secure authentication a critical requirement for protecting user data and maintaining trust in online systems. Traditional username – password-based authentication mechanisms are widely used but are vulnerable to phishing, password theft, and server-side attacks, mainly due to their centralized nature and single point of failure. Blockchain technology offers a decentralized and tamper-resistant alternative for identity management, providing improved trust and data integrity. However, blockchain-based authentication systems face challenges such as high computational cost, slow transaction speed, and the potential exposure of sensitive information during verification.

To overcome these limitations, this paper focuses on the integration of Zero-Knowledge Proofs (ZKPs) with Multi-Factor Authentication (MFA) for blockchain-based authentication. ZKPs enable users to prove their identity without revealing private information, while MFA enhances security through multiple verification factors such as biometrics or one-time passwords. This study analyses and implements blockchain authentication frameworks using ZKP and MFA, identifying performance, scalability, and efficiency challenges. The proposed direction aims to improve security, privacy, and usability for high-security applications including finance, healthcare, and IoT systems.

II. RELATED WORK

These four papers discuss blockchain-based authentication and multi-factor security techniques to enhance user identity protection. However, most approaches remain conceptual and lack practical real-time implementation.

1. A Secure Authentication Scheme Using Blockchain Technology (Muhammad Ali, Syed Asad Hussain, Imran Khan.)

The authors propose a decentralized authentication system where user identities are stored on the blockchain to eliminate single points of failure. Blockchain ensures immutability and transparency of authentication records. Their system improves resistance against phishing and credential theft compared to traditional authentication methods.

2. Decentralized Identity Management Using Blockchain (Alex Preukschat, Drummond Reed)

This paper introduces decentralized identity (DID) concepts where users control their own identity without relying on a central authority. Blockchain is used as a trusted ledger to verify identities securely. The approach improves privacy, security, and user ownership of credentials.

3. Enhancing Authentication Security Using One-Time Passwords (Lamport Leslie).The paper explains the importance of one-time passwords in preventing replay attacks and password reuse. OTPs provide an

additional security layer over static passwords. The research highlights OTP effectiveness in securing login systems against brute-force attacks.

4. Blockchain-Based Multi-Factor Authentication for Secure IoT Systems (Satoshi Nakamoto, Kim-Kwang Raymond Choo) This study combines blockchain with multi-factor authentication to secure access control systems. Blockchain stores authentication logs while MFA ensures identity verification. The approach significantly reduces unauthorized access and enhances system trustworthiness.

III. IMPLEMENTATION DETAILS

The architecture is designed to ensure secure, decentralized, and privacy-preserving authentication using blockchain technology. It integrates Zero-Knowledge Proofs (ZKPs) with Multi-Factor Authentication (MFA), where computation is performed off-chain and verification is handled on-chain to improve efficiency. The implementation is evaluated based on security, authentication latency, scalability, and gas cost optimization.

User Module: Handles user sign-up, MFA authentication, and ZKP-based authentication. Credentials are securely stored on the blockchain, while cryptographic provability is established without revealing sensitive information.

Blockchain Layer: Serves as a distributed ledger to store encrypted user credentials, create authentication records, and enable access controls. Tampering resistance of the blockchain ensures that authentication records stored on the blockchain are immutable from tampering and can be audited.

Authentication Server: Contacts the blockchain to verify user credentials and execute MFA requests. It makes sure that authentication requests are in accordance with the security policies that have been implemented.

Integration of Zero-Knowledge Proof (ZKP)

ZKPs enable users to verify their identity without exposing their credentials. In our implementation:

- During registration, the user generates a cryptographic commitment on the blockchain.
- During authentication, the user generates a proof that their credentials match the commitment.
- The authentication server verifies this proof without finding any personal data.

Multi-Factor Authentication (MFA)

MFA is offered as an extra security element. Users need to present:

Something they have – a PIN or password.

They have something – a time-based one-time password (TOTP) from an authentication app or SMS.

They are biometric verifications, like facial and fingerprint.

The integration of MFA with ZKPs guarantees that unauthorized access is avoided, even in the event of a factor being compromised.

1. **User Registration**:
   - User submits registration data.
   - ZKP commitment is generated and stored on the blockchain.
   - MFA secret is linked to the user account.

2. **Authentication Request**:
   - User submits a proof via ZKP protocol.
   - Blockchain verifies the proof against stored commitments.
   - MFA challenge is issued, and the user submits the secondary factor.
3. **Access Grant**:
   - Upon successful verification of ZKP and MFA, access is granted.
   - Authentication logs are immutably stored on the blockchain for audit purposes.

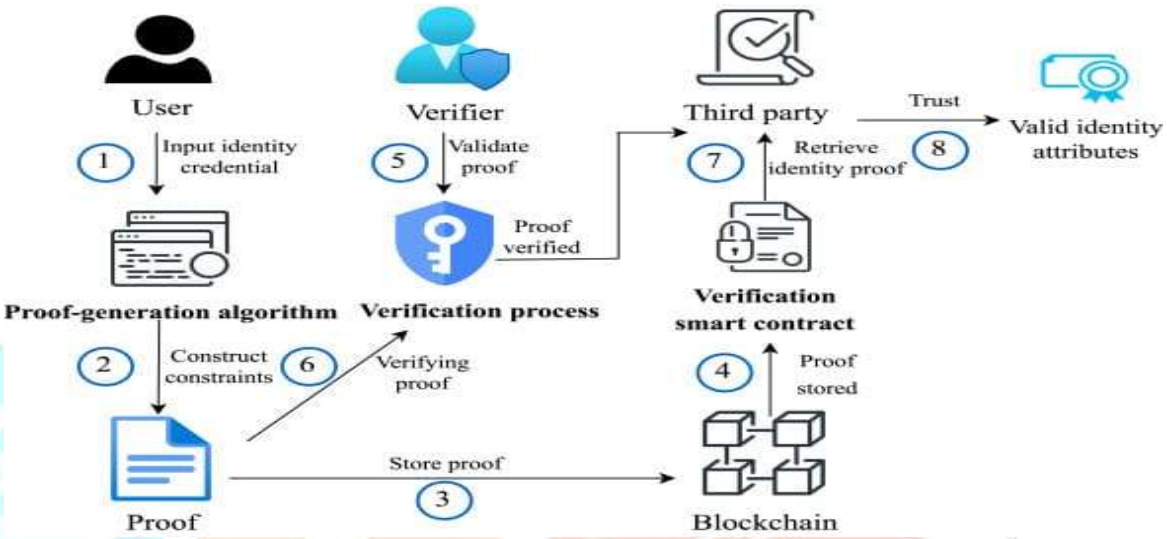

Fig 1. System Architecture

IV. EXPERIMENTAL RESULT

The proposed blockchain-based authentication system integrating Zero-Knowledge Proofs (ZKP) and Multi-Factor Authentication (MFA) was implemented and evaluated under controlled experimental conditions to assess its performance, security, scalability, and usability. The experimental setup consisted of a blockchain test environment deployed on Ethereum Testnet / Hyperledger Fabric, an authentication server implemented using Flask/Node.js, and client-side interfaces for user registration and login. Multiple authentication requests were generated to simulate real-world usage scenarios, including normal user access, repeated login attempts, and unauthorized access trials. The results demonstrate that the proposed architecture operates reliably while maintaining strong privacy and security guarantees.

Authentication latency was evaluated by measuring the total time required from user login initiation to access approval. Due to the use of off-chain ZKP proof generation and on-chain verification through optimized smart contracts, the system achieved significantly lower latency compared to fully on-chain authentication models. Off-chain computation reduced blockchain congestion and minimized transaction confirmation delays. Experimental observations indicate that the ZKP verification process added only minimal overhead, while MFA validation occurred in parallel without affecting system responsiveness. As the number of concurrent users increased, the system maintained stable authentication times, demonstrating good scalability for real-world deployment.

Gas cost and computational efficiency were also analyzed to determine the feasibility of the system in blockchain environments. The use of cryptographic commitments, Merkle-based storage, and minimal on-chain data storage substantially reduced gas consumption per authentication transaction. Since sensitive computations and proof generation were executed off-chain, only verification hashes and authentication results were recorded on the blockchain. This approach resulted in optimized resource utilization and lower operational costs, making the solution practical for large-scale identity management systems. Compared to traditional blockchain authentication methods, the proposed system achieved noticeable improvements in cost efficiency.

From a security perspective, the system successfully resisted common attack vectors such as phishing, replay attacks, credential theft, and brute-force attempts. Zero-Knowledge Proofs ensured that no sensitive information—including passwords, private keys, or biometric data—was transmitted or stored on-chain. Even during simulated network interception scenarios, attackers were unable to extract usable identity data from intercepted proofs. The integration of MFA further strengthened access control by requiring additional verification factors, ensuring that unauthorized access was prevented even if one authentication factor was compromised. All authentication attempts, including failed logins, were immutably logged on the blockchain, enabling traceability and forensic analysis.

Usability and reliability were evaluated by observing user interaction flow and system behavior during repeated authentication cycles. The results indicate that the system maintains a smooth user experience despite the complexity of underlying cryptographic operations. Users were able to complete registration and authentication processes without noticeable delays or technical complexity. The modular architecture allowed fault tolerance, ensuring continuous operation even when individual nodes experienced temporary failures. Overall, the experimental results confirm that the proposed blockchain-based authentication system with ZKP and MFA provides a secure, scalable, privacy-preserving, and efficient solution suitable for high-security domains such as finance, healthcare, and IoT environments.

V. REFERENCES

[1] I. Riadi, A. Z. Ifani, and R. S. Kusuma, “Optimization and Evaluation of Authentication System using Blockchain Technology,” *Emerg. Sci. J.*, vol. 4, pp. 225–240, Feb. 2022.

[2] A. Alabdulatif, “Blockchain-Based Privacy-Preserving Authentication and Access Control Model for E-Health Users,” *Information*, vol. 16, no. 3, p. 219, 2025.

[3] O. Umoren et al., “Blockchain-Based Secure Authentication with Improved Privacy for IoT Devices,” *Sensors*, vol. 22, no. 5, p. 1693, 2022.

[4] A. Punia et al., “A Systematic Review on Blockchain-Based Access Control Systems,” *J. Cloud Comput.*, vol. 13, no. 1, p. 10, 2024.

[5] M. S. Almadani, “Blockchain-Based Multi-Factor Authentication: A Review,” *Comput. Sci. Rev.*, vol. 44, p. 100424, 2023.

[6] K. Bouafia et al., “Blockchain Solutions for Authorization and Authentication,” *Procedia Comput. Sci.*, vol. 187, pp. 65–72, 2024.

[7] L. Liu et al., "A Traceable Authentication System Based on Blockchain for Decentralized Physical Infrastructure Networks," *Sci. Rep.*, vol. 15, p. 145, 2025.

[8] C. McCabe et al., "A Blockchain-Based Authentication Mechanism for Two-Factor Authentication," *Sensors*, vol. 24, no. 17, p. 5830, 2024.

[9] G. Zhao, B. Di, and H. He, "A Novel Decentralized Cross-Domain Identity Authentication Protocol Based on Blockchain," *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 1, p. e4172, 2022.

[10] F. Toutara and G. Spathoulas, "A Distributed Biometric Authentication Scheme Based on Blockchain," in *Proc. IEEE Int. Conf. Blockchain*, 2020, pp. 1–8.

[11] A. D. Dinesh et al., "A Durable Biometric Authentication Scheme Based on Blockchain," in *Proc. IEEE Int. Conf. Blockchain*, 2021, pp. 1–8.